

What is claimed is:

- 1 1. A system for securely authenticating a data exchange session with
2 an implantable medical device, comprising:
3 a crypto key uniquely associated with an implantable medical device to
4 authenticate data during a data exchange session; and
5 an external source to establish a secure connection with a secure key
6 repository to securely maintain the crypto key, and to authenticate authorization to
7 access data on the implantable medical device by securely retrieving the crypto
8 key from the secure key repository.
- 1 2. A system according to Claim 1, wherein the external source
2 transacts a data exchange session using the crypto key to authenticate the data.
- 1 3. A system according to Claim 2, further comprising:
2 an authentication component to employ the crypto key during the data
3 exchange session, comprising at least one of:
4 a command authenticator to authenticate commands exchanged
5 through the external source with the implantable medical device and ;
6 a data integrity checker to check the integrity of the data received
7 by and transmitted from the external source; and
8 a data encrypter to encrypt the data received by and transmitted
9 from the external source.
- 1 4. A system according to Claim 1, further comprising:
2 a short range interface logically defining a secured area around the
3 implantable medical device in which to establish the secure connection; and
4 a long range interface logically defining a non-secured area extending
5 beyond the secured area in which to transact the data exchange session.
- 1 5. A system according to Claim 1, further comprising:
2 a key generator to statically generate the crypto key, and to persistently
3 store the crypto key in the secure key repository.

1 6. A system according to Claim 5, wherein the crypto key is stored on
2 at least one of the implantable medical device, a patient designator, a secure
3 database, a physical token, and a repeater.

1 7. A system according to Claim 5, wherein the crypto key is securely
2 retrieved from the secure key repository through a programmer.

1 8. A system according to Claim 1, further comprising:
2 a key generator to dynamically generate the crypto key.

1 9. A system according to Claim 8, wherein the crypto key is stored on
2 at least one of the implantable medical device, a patient designator, and a repeater.

1 10. A system according to Claim 8, wherein the crypto key is securely
2 retrieved from the secure key repository through at least one of a programmer and
3 a repeater.

1 11. A system according to Claim 1, wherein the crypto key is
2 maintained on the implantable medical device, further comprising:
3 a short range telemetry interface retrieving the crypto key through short
4 range telemetry.

1 12. A system according to Claim 11, wherein the short range telemetry
2 comprises inductive telemetry.

1 13. A system according to Claim 11, wherein the external source
2 comprises a programmer.

1 14. A system according to Claim 13, wherein the crypto key is
2 provided from the programmer to a repeater.

1 15. A system according to Claim 11, wherein the external source
2 comprises a patient designator.

1 16. A system according to Claim 15, wherein the crypto key is
2 provided from the patient designator to at least one of a programmer and a
3 repeater.

1 17. A system according to Claim 1, further comprising:
2 a secure database to maintain the crypto key; and
3 a secure server providing the crypto key through a secure connection.

1 18. A system according to Claim 17, wherein the secure connection
2 comprises at least one of a serial or hardwired connection and a secure network
3 connection.

1 19. A system according to Claim 17, wherein the external source
2 comprises a programmer.

1 20. A system according to Claim 19, wherein the crypto key is
2 provided from the programmer to a repeater.

1 21. A system according to Claim 1, further comprising:
2 a physical token to maintain the crypto key; and
3 a reader to retrieve the crypto key by accessing the physical token.

1 22. A system according to Claim 21, further comprising:
2 a physical label to specify the crypto key on the physical token.

1 23. A system according to Claim 22, wherein the physical label
2 comprises at least one of alphanumeric text, bar coding, and an outwardly-
3 appearing indication.

1 24. A system according to Claim 21, further comprising:
2 internal storage to specify the crypto key on the physical token.

1 25. A system according to Claim 24, wherein the internal storage
2 comprises at least one of a transistor, a memory circuit, an electronically readable
3 storage medium, and a magnetically readable storage medium.

1 26. A system according to Claim 21, wherein the physical token is
2 accessed using magnetic, optical, serial, and physical reading.

1 27. A system according to Claim 1, wherein the crypto key comprises
2 at least one of a 128-bit crypto key and a symmetric crypto key.

1 28. A system according to Claim 1, wherein the crypto key comprises
2 at least one of a statically generated and persistently stored crypto key,
3 dynamically generated and persistently stored crypto key, a dynamically
4 generated and non-persistently stored session crypto key.

1 29. A system according to Claim 1, wherein implantable medical
2 device comprises at least one of an implantable cardiac device, neural stimulation
3 device, and drug therapy dispensing device.

1 30. A method for securely authenticating a data exchange session with
2 an implantable medical device, comprising:
3 defining a crypto key uniquely associated with an implantable medical
4 device to authenticate data during a data exchange session;
5 establishing a secure connection from an external source with a secure key
6 repository securely maintaining the crypto key; and
7 authenticating authorization to access data on the implantable medical
8 device by securely retrieving the crypto key from the secure key repository.

1 31. A method according to Claim 30, further comprising:
2 transacting a data exchange session through the external source using the
3 crypto key to authenticate the data.

1 32. A method according to Claim 31, further comprising:

2 employing the crypto key during the data exchange session, comprising at
3 least one of:
4 authenticating commands exchanged through the external source
5 with the implantable medical device and ;
6 checking the integrity of the data received by and transmitted from
7 the external source; and
8 encrypting the data received by and transmitted from the external
9 source.

1 33. A method according to Claim 30, further comprising:
2 logically defining a secured area around the implantable medical device in
3 which to establish the secure connection; and
4 logically defining a non-secured area extending beyond the secured area in
5 which to transact the data exchange session.

1 34. A method according to Claim 30, further comprising:
2 statically generating the crypto key; and
3 persistently storing the crypto key in the secure key repository.

1 35. A method according to Claim 34, wherein the crypto key is stored
2 on at least one of the implantable medical device, a patient designator, a secure
3 database, a physical token, and a repeater.

1 36. A method according to Claim 35, further comprising:
2 securely retrieving the crypto key from the secure key repository through a
3 programmer.

1 37. A method according to Claim 30, further comprising:
2 dynamically generating the crypto key.

1 38. A method according to Claim 37, wherein the crypto key is stored
2 on at least one of the implantable medical device, a patient designator, and a
3 repeater.

1 39. A method according to Claim 37, further comprising:
2 securely retrieving the crypto key from the secure key repository through
3 at least one of a programmer and a repeater.

1 40. A method according to Claim 30, further comprising:
2 maintaining the crypto key on the implantable medical device; and
3 retrieving the crypto key through short range telemetry.

1 41. A method according to Claim 40, wherein the short range
2 telemetry comprises inductive telemetry.

1 42. A method according to Claim 40, wherein the external source
2 comprises a programmer.

1 43. A method according to Claim 42, further comprising:
2 providing the crypto key from the programmer to a repeater.

1 44. A method according to Claim 40, wherein the external source
2 comprises a patient designator.

1 45. A method according to Claim 44, further comprising:
2 providing the crypto key from the patient designator to at least one of a
3 programmer and a repeater.

1 46. A method according to Claim 30, further comprising:
2 maintaining the crypto key in a secure database; and
3 retrieving the crypto key through a secure connection.

1 47. A method according to Claim 46, wherein the secure connection
2 comprises at least one of a serial or hardwired connection and a secure network
3 connection.

1 48. A method according to Claim 46, wherein the external source
2 comprises a programmer.

- 1 49. A method according to Claim 48, further comprising:
2 providing the crypto key from the programmer to a repeater.
- 1 50. A method according to Claim 30, further comprising:
2 maintaining the crypto key on a physical token; and
3 retrieving the crypto key by accessing the physical token.
- 1 51. A method according to Claim 50, further comprising:
2 specifying the crypto key on the physical token using a physical label.
- 1 52. A method according to Claim 51, wherein the physical label
2 comprises at least one of alphanumeric text, bar coding, and an outwardly-
3 appearing indication.
- 1 53. A method according to Claim 50, further comprising:
2 specifying the crypto key on the physical token using internal storage.
- 1 54. A method according to Claim 53, wherein the internal storage
2 comprises at least one of a transistor, a memory circuit, an electronically readable
3 storage medium, and a magnetically readable storage medium.
- 1 55. A method according to Claim 50, further comprising:
2 accessing the physical token using magnetic, optical, serial, and physical
3 reading.
- 1 56. A method according to Claim 30, wherein the crypto key
2 comprises at least one of a 128-bit crypto key and a symmetric crypto key.
- 1 57. A method according to Claim 30, wherein the crypto key
2 comprises at least one of a statically generated and persistently stored crypto key,
3 dynamically generated and persistently stored crypto key, a dynamically
4 generated and non-persistently stored session crypto key.

1 58. A method according to Claim 30, wherein implantable medical
2 device comprises at least one of an implantable cardiac device, neural stimulation
3 device, and drug therapy dispensing device.

1 59. An apparatus for securely authenticating a data exchange session
2 with an implantable medical device, comprising:
3 means for defining a crypto key uniquely associated with an implantable
4 medical device to authenticate data during a data exchange session;
5 means for establishing a secure connection from an external source with a
6 secure key repository securely maintaining the crypto key; and
7 means for authenticating authorization to access data on the implantable
8 medical device by means for securely retrieving the crypto key from the secure
9 key repository.

1 60. A system for securely transacting a data exchange session with an
2 implantable medical device, comprising:
3 a short range interface to provide communication with an implantable
4 medical device by authenticating access to a securely maintained crypto key;
5 a long range interface to commence a data exchange session upon
6 successful access authentication with the implantable medical device, and to
7 transact the data exchange session using the crypto key.

1 61. A system according to Claim 60, wherein the patient health
2 information is maintained in an encrypted form.

1 62. A system according to Claim 60, wherein the authenticating with
2 the implantable medical device is through short range telemetry, further
3 comprising:
4 a short range telemetric connection with the implantable medical device;
5 a short range telemetric device to request the crypto key from the
6 implantable medical device, and to receive the crypto key from the implantable
7 medical device.

1 63. A system according to Claim 60, wherein the authenticating with
2 the implantable medical device is through a patient designator, further
3 comprising:

4 a short range telemetric connection with the implantable medical device;
5 a patient designator to request the crypto key from the implantable
6 medical device, and to receive the crypto key from the implantable medical
7 device.

1 64. A system according to Claim 60, wherein the authenticating with
2 the implantable medical device is by using a physical token, further comprising:

3 a physical token; and
4 a reader to receive the crypto key from the physical token.

1 65. A system according to Claim 60, wherein the patient health
2 information is maintained in the implantable medical device in unencrypted form
3 and is accessible in the unencrypted form exclusively through a short range
4 telemetric connection.

1 66. A system according to Claim 65, wherein the authenticating with
2 the implantable medical device is through short range telemetry, further
3 comprising:

4 a short range telemetric connection with the implantable medical device;
5 an external source to send a session crypto key to the implantable medical
6 device; and
7 an encrypter to encrypt the patient health information maintained in the
8 implantable medical device.

1 67. A system according to Claim 60, wherein the authenticating with
2 the implantable medical device is through a patient designator, further
3 comprising:

4 a patient designator to establish a short range telemetric connection with
5 the implantable medical device, and to send a session crypto key to the
6 implantable medical device; and
7 an encrypter to encrypt the patient health information maintained in the
8 implantable medical device.

1 68. A system according to Claim 60, wherein the long range interface
2 is augmented using one or more repeaters.

1 69. A method for securely transacting a data exchange session with an
2 implantable medical device, comprising:
3 providing communication with an implantable medical device by
4 authenticating access to a securely maintained crypto key using a short range
5 interface;
6 commencing a data exchange session by transitioning to long range
7 interface upon successful access authentication with the implantable medical
8 device; and
9 transacting the data exchange session using the crypto key.

1 70. A method according to Claim 69, wherein the patient health
2 information is maintained in an encrypted form.

1 71. A method according to Claim 69, wherein the authenticating with
2 the implantable medical device is through short range telemetry, further
3 comprising:
4 establishing a short range telemetric connection with the implantable
5 medical device;
6 requesting the crypto key from the implantable medical device; and
7 receiving the crypto key from the implantable medical device.

1 72. A method according to Claim 69, wherein the authenticating with
2 the implantable medical device is through a patient designator, further
3 comprising:

4 establishing a short range telemetric connection between the implantable
5 medical device and the patient designator;
6 requesting for the crypto key from the implantable medical device; and
7 receiving the crypto key from the implantable medical device.

1 73. A method according to Claim 69, wherein the authenticating with
2 the implantable medical device is by using a physical token, further comprising:
3 accessing the physical token; and
4 receiving the crypto key from the physical token.

1 74. A method according to Claim 69, wherein the patient health
2 information is maintained in the implantable medical device in unencrypted form
3 and is accessible in the unencrypted form exclusively through a short range
4 telemetric connection.

1 75. A method according to Claim 74, wherein the authenticating with
2 the implantable medical device is through short range telemetry, further
3 comprising:
4 establishing a short range telemetric connection with the implantable
5 medical device;
6 sending a session crypto key to the implantable medical device; and
7 encrypting the patient health information maintained in the implantable
8 medical device.

1 76. A method according to Claim 69, wherein the authenticating with
2 the implantable medical device is through a patient designator, further
3 comprising:
4 establishing a short range telemetric connection with the implantable
5 medical device through the patient designator;
6 sending a session crypto key to the implantable medical device; and
7 encrypting the patient health information maintained in the implantable
8 medical device.

1 77. A method according to Claim 69, wherein the long range interface
2 is augmented using one or more repeaters.

1 78. An apparatus for securely transacting a data exchange session with
2 an implantable medical device, comprising:

3 means for providing communication with an implantable medical device
4 by means for authenticating access to a securely maintained crypto key using a
5 short range interface;

6 means for commencing a data exchange session by means for transitioning
7 to long range interface upon successful access authentication with the implantable
8 medical device; and

9 means for transacting the data exchange session by accessing patient
10 health information stored on the implantable medical device using the crypto key.

1 79. A system for securely transacting a data exchange session with an
2 implantable medical device through secure lookup, comprising:

3 a secure server to provide identification of and authentication to access an
4 implantable medical device by authenticating access to a securely maintained
5 crypto key;

6 a secure external source to request the crypto key via a secure connection
7 based on the identification of and authentication to access the implantable medical
8 device, and to receive the crypto key; and

9 a long range interface to commence a data exchange session upon
10 successful access authentication with the implantable medical device, and to
11 transact the data exchange session using the crypto key.

1 80. A method for securely transacting a data exchange session with an
2 implantable medical device through secure lookup, comprising:

3 providing identification of and authentication to access an implantable
4 medical device by authenticating access to a securely maintained crypto key;

5 requesting the crypto key via a secure connection based on the
6 identification of and authentication to access the implantable medical device; and

7 receiving the crypto key;
8 commencing a data exchange session by transitioning to long range
9 interface upon successful access authentication with the implantable medical
10 device; and
11 transacting the data exchange session using the crypto key.

1 81. An apparatus for securely transacting a data exchange session with
2 an implantable medical device through secure lookup, comprising:
3 means for providing identification of and authentication to access an
4 implantable medical device by means for authenticating access to a securely
5 maintained crypto key;
6 means for requesting the crypto key via a secure connection based on the
7 identification of and authentication to access the implantable medical device; and
8 means for receiving the crypto key;
9 means for commencing a data exchange session by means for transitioning
10 to long range interface upon successful access authentication with the implantable
11 medical device; and
12 means for transacting the data exchange session using the crypto key.